



Government Information Technology Agency

NOI Encryption Readiness Checklist

Agency Name: _____

NOI ID: Agency AFIS ID (XXX) + date (mm/dd/yyyy): _____

Contact Information: Name: _____

E-mail: _____ Phone: _____

NO responses to any checklist item require a written explanation attachment

I, hereby confirm that my agency, board or commission understands and complies with the spirit and intent of [HB 2785, Section 23](#), [Executive Order 2008-10](#) and [ARS 41-3507](#). ☐ Yes ☐ No

In addition I take responsibility for the following, and confirm that my organization adheres to the [Statewide IT Polices, Standards and Practices](#) when implementing encryption solutions:

1. Has attached a brief written description of proposed encryption solution(s): ☐ Yes ☐ No
2. Proposed encryption solution has been reviewed and approved by agency Director, Information Security Officer and Privacy Officer: ☐ Yes ☐ No
3. Is a PIJ required for proposed encryption solution(s): ☐ Yes ☐ No
4. Has a dedicated Project Manager responsible for assessment and implementation of proposed solution been assigned? ☐ Yes ☐ No
5. Will the services of an IT security consultant be utilized in the evaluation and/or implementation of proposed solution? ☐ Yes ☐ No
6. Complies with statewide P170 Privacy policy: ☐ Yes ☐ No
7. Complies with statewide P740 - S741 *Classification and Categorization of Data Standard*: ☐ Yes ☐ No
8. Complies with statewide S850 *Encryption Standard*: ☐ Yes ☐ No
9. Have addressed "Key" management roles and responsibilities: ☐ Yes ☐ No
10. Has agency's "Acceptable Use" policy (statement) been updated to incorporate use of encryption technology and required business practices by agency staff and key 3rd parties? ☐ Yes ☐ No
11. Have all agency computer systems user's (e.g., state employees, interns, volunteers, vendors, contactors, etc.) been trained and signed the updated "Acceptable Use" policy? ☐ Yes ☐ No



Government Information Technology Agency

12. Which encryption solution(s) are being proposed for implementation?

- a. Full Disk: File Encryption: ☐ Yes ☐ No
- b. Back-up Media and Archiving: ☐ Yes ☐ No
- c. Mass Storage (SANs, NAS Encryption): ☐ Yes ☐ No
- d. Database Encryption: ☐ Yes ☐ No
- e. Removable Storage Drives and Devices: ☐ Yes ☐ No
- f. Secured Transport of Information: ☐ Yes ☐ No
- g. IT Security Consulting Services: ☐ Yes ☐ No

13. Has agency identified the total implementation cost for hardware, software, staff training, licensing and professional services for the proposed encryption solution(s)? ☐ Yes ☐ No

14. Has agency identified the on-going maintenance cost for hardware, software, staff training, licensing and professional services for the proposed encryption solution(s)? ☐ Yes ☐ No

15. Have minimum personal information encryption requirements as set forth in [HB 2785, Section 23](#), been addressed or protected by the proposed encryption solution? ** ☐ Yes ☐ No

16. Manages HIPAA and any personal identifiable information (for citizens, third parties and state employees) as confidential data, classifying and storing in a secured/encrypted environment: ☐ Yes ☐ No

** [HB 2785, Section 23](#) defines personal information as: an individual's first name or first initial and last name in combination with any one of the following: Social Security Number, Drivers License, Identification card number, Account Number, Credit or Debit Card Number, Security Code, Access Code or Password.

Submitted By _____
Printed Name Signature

Administrative/ _____
Technical Review Printed Name Signature

Approved _____
CISO/CPO Printed Name Signature

State CIO Approval Letter Issued (Attached) _____
Date Issued

Agency Completion Letter Received _____
Date Received